ADHOC 168
13 May 2006; Disk Used
ARTICLE IN PRESS
No. of Pages 13, Model 3+

Available online at www.sciencedirect.com

Ad Hoc Networks xxx (2006) xxx–xxx

www.elsevier.com/locate/adhoc

Analysis of area-congestion-based DDoS attacks in ad hoc networks

Qijun Gu [a], Peng Liu [b,*], Chao-Hsien Chu [b]

[a] *Department of Computer Science, Texas State University, San Marcos, TX 78666, United States*
[b] *School of Information Sciences and Technology, Pennsylvania State University, 313G IST Building, University Park, Pennsylvania, PA 16802, United States*

Received 8 September 2004; received in revised form 28 September 2005; accepted 11 April 2006

Abstract

Increased instances of distributed denial of service (DDoS) attacks on the Internet have raised questions on whether and how ad hoc networks are vulnerable to such attacks. This paper studies the special properties of such attacks in ad hoc networks. We examine two types of area-congestion-based DDoS attacks – remote and local attacks – and present in-depth analysis on various factors and attack constraints that an attacker may use and face. We find that (1) there are two types of congestion – self congestion and cross congestion – that need to be carefully monitored; (2) the normal traffic itself causes significant packet loss in addition to the attack impacts in both remote and local attacks; (3) the number of flooding nodes has major impacts on remote attacks while, the load of normal traffic and the position of flooding nodes are critical to local attacks; and (4) given the same number of flooding nodes and attack loads, a remote DDoS attack can cause more damage to the network than a local DDoS attack.

Keywords: Ad hoc network; Security; Congestion; Distributed denial of service; Denial of service

1. Introduction

DDoS attacks present a serious threat to network computing and have recently attracted much attention [1–6]. When a DDoS attack is launched, a large number of hosts controlled by the attackers flood a target with a high volume of packets to significantly degrade the target's service performance or render it unable to deliver any service. Ad hoc networks differ from the Internet in several critical ways that make them especially vulnerable to DDoS attacks. First, ad hoc nodes are peers. Because of this, once an attacker compromises a node, they can attack the network from inside. Second, every node in an ad hoc network is not only a host but also a router. Thus, it is harder to determine whether a suspicious packet is from an attacker or relayed from a legitimate node. These features indicate that there may be "easier" ways to cause denial of service (DoS) in ad hoc networks than in the Internet, and that existing Internet DDoS defense mechanisms may not be enough to counter DDoS attacks in ad hoc networks.

* Corresponding author. Tel.: +1 814 863 0641.
E-mail address: pliu@ist.psu.edu (Q. Gu).

1570-8705/$ - see front matter © 2006 Published by Elsevier B.V.
doi:10.1016/j.adhoc.2006.04.002

Although congestion was recognized as a simple and effective DoS attack approach in ad hoc networks, previous studies mainly focused on individual attackers and the attack impacts on individual nodes and traffic flows. In an ad hoc network, it is easy for attackers to attack simultaneously from distributed locations; however, it is not clear how damaging the attacks can be and what are the unique characteristics of the attacks. Due to the relative newness of these concerns, more research on the properties and methods of DDoS attacks in ad hoc networks is needed.

Motivated by these observations, we explore the possible DDoS attacks and their impacts on ad hoc networks. In particular, we investigate how attackers flood legitimate routes with junk packets. Because wireless bandwidth is limited, the junk packets can easily cause severe wireless channel contention among nearby nodes on the legitimate routes. Therefore, the attack creates network-wide congestion instead of congestion surrounding only the destination as in conventional Internet DDoS attacks. In this paper, we explore and discuss two types of congestion – self and cross congestions – that may be caused by attacks. We analyze the important factors that may affect the attacks. We also review the existing defense mechanisms against these DDoS attacks. This research lays the necessary foundation for developing more effective defense strategies against DDoS attacks in ad hoc networks.

2. Background

In this section, we present background information on DDoS and DoS attacks and review related works.

2.1. DDoS attacks

In the Internet, attackers can launch a DDoS attack from a huge number of hosts to conquer a few target servers. Many attacking approaches have been identified. For example, attackers can send a flood of SYN packets to block one of the server's TCP ports [7], flood the targets with misformed ICMP echo packets [8], or bruteforcely flood them with UDP packets [9]. Since most flooding packets in DDoS attacks are sent out with spoofed source addresses, much research on defense has focused on identifying the true flooding sources, tracing back to those sources, and filtering out the flooding packets. Aura et al. [10] proposed letting the server ask the client to respond to a cookie or solve a puzzle when the client requests connection to the server. If the client is spoofed, no reply will come from a spoofed machine, or the real attacker will be overwhelmed by the server's response requests. Ferguson et al. [1] proposed the ingress filtering technology to filter packets with a spoofed address outside the attacker's network. Mirkovic et al. [4] proposed D-WARD to set a rate limit for a suspicious flow that does not match its normal model. With the help of routers that embed trace information in a number of normal packets, the victim can figure out the real attack sources based on trace back [2,11]. Pi [5] lets the victim identify the flooding source by putting unique path identifiers in packets. Push back [3,12] identifies attack aggregates in congested routers. SAVE [13] requires routers to verify the source address of incoming packets. In SIFF [6], routers manipulate the marking fields in packets so that an end-host can selectively stop individual flows from reaching its network. A comprehensive overview and classification of DDoS attacks and defense approaches can be found in [14].

A major characteristic of DDoS attacks in the Internet is that the attacking sources are end hosts that connect to the Internet from their access networks and are remote to the victim. To take over the target, the flooding packets travel through the Internet from the flooding sources to the target. In an ad hoc network, this kind of attack approach is not the only choice for attackers. Since ad hoc nodes are inside the network, the attackers are closer to the target and can directly congest it. The attackers can also redirect and forward traffic to the target instead of generating junk packets by themselves. In addition, because mobile nodes are no longer the end hosts in an ad hoc network, attackers can bypass the defending nodes. Hence, it is important to clearly understand the possible new features of such attacks and how DDoS attacks can be prevented in an ad hoc network.

2.2. DoS attacks in ad hoc networks

There are many approaches to launching DoS attacks in an ad hoc network. In the physical layer, jamming can be used to disrupt and suppress normal transmission [15]. In the MAC layer, the attackers can exploit defects of MAC protocol messages and procedures. For instance, in the 802.11 MAC protocol, the attackers can provide bogus duration information or misuse the carrier sense mechanism to deceive normal nodes to avoid collision or keep silent [16]. Gu et al. [17] analyzed how the attackers can use certain packet generation and transmission behavior to obtain more bandwidth than legitimate nodes so that legitimate transmission is suppressed. Wullems et al. [18] identified a weakness in the current MAC protocol that enables an attacker to deceive other nodes and stop transmission. The attackers can exploit the CCA function of the 802.11 PHY protocol to suppress other nodes with the illusion of a busy channel. Borisov et al. [19] discovered several security flaws in WEP, which enables an attacker to modify a message without being detected and prevent users from obtaining correct information from their service provider. Authors from Refs. [20–23] have found that attackers can break valid routes and connections by manipulating routing procedures and packets. Aad et al. [20] identified the JellyFish attacks that drop, reorder or delay TCP packets to disrupt TCP connections.

Differing from DDoS attack approaches in the Internet, the aforementioned DoS attack approaches, except those that deal with routing or higher layers, generally require an attacker to have a specially designed network card in order to compose the attacking packets. For example, the attacker needs to generate a strong signal in the bandwidth for jamming, composing special MAC packets for channel congestion, modifying forwarded routing packets to detour routes, or disordering TCP packets to break TCP connections. Hence, these approaches are not very practical for attackers trying to launch attacks from compromised nodes. In this paper, we study a simple attack approach where attackers inject packets into legitimate routes. This approach only requires an attacking node to get valid routes from its routing tables and impersonate a legitimate node.

3. Area-congestion-based DDoS attacks

Congestion has been recognized as a simple and effective DoS attack approach in ad hoc networks. In this section, we examine the special features and concerns of area-congestion-based DDoS attacks.

3.1. Attack topologies

We classify the DDoS attacks into *remote attacks* and *local attacks*, according to attack topologies. Fig. 1 depicts the topologies and possible congestion resulting from the DDoS attacks. The gray elliptical area is an ad hoc network, where nodes $a1$, $a2$, and $a3$ are the attackers, and nodes $n1$, $n2$, and $n3$ are the legitimate nodes. The dashed lines stand for the attack traffic through multiple hops, and the solid lines for the attack traffic to nearby nodes. The shadowed areas are possible congested areas.

The remote attacks in ad hoc networks are different from flooding in the Internet. In the Internet, a congested link keeps its maximum throughput during each attack period. However, in ad hoc networks, because the communication channel is open and shared, packets in a small area can collide with each other. Hence, different attack streams interfere with each other when they go through the same area. In addition, an attack stream may experience self-congestion and the route may frequently change during the attack. As a consequence, which routing nodes may forward the flooding packets and how many flooding packets can reach the target through multiple hops are largely unpredictable. Our simulations (described in detail later) show that in a remote DDoS attack more flooding nodes and higher attack load may in fact reduce the attack impacts.

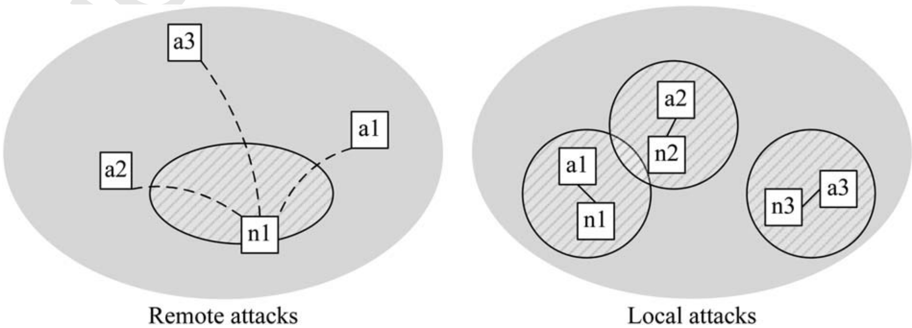


Fig. 1. Area-congestion-based attacks.

Since local attackers are competing for the channel with all other nearby nodes, local attackers may suffer less self-congestion and be able to cause more congestion to nearby targets. Our simulations show that the impact of a local DDoS attack increases with more flooding nodes and higher attack loads. However, given the same number of flooding nodes and attack loads, a remote DDoS attack can cause more damage to the network than a local DDoS attack.

3.2. Attackers

Similar to DDoS attacks in the Internet, area-congestion-based attacks need enough flooding sources to significantly degrade the service performance. One approach for attackers in an ad hoc network to obtain flooding nodes is to compromise vulnerable mobile nodes or deploy mobile nodes in different locations before the event. With enough flooding nodes, compromised or deployed, the attackers can command these nodes to flood the network at the appropriate time.

However, a flooding node may face other challenges among which energy constraint is the most critical one, especially when the flooding node is a compromised mobile node. Since flooding consumes power, a DDoS attack may not be economical if the attack impact is not devastating. However, we find that it does not require many flooding nodes or high attack loads to cause serious damage. Furthermore, the damage of a DDoS attack is mainly determined by how the network is used and how users experience the attack. In some critical situations, such as in a battlefield, DDoS attackers may be willing to trade energy to take over the ad hoc network even for only a short period. In addition, if the flooding sources secretly tap into power sources, energy constraints may not be an issue.

4. Remote attacks

In this section, we describe how an attacker can inject packets into legitimate routes without being detected. We also analyze the characteristics of remote attacks, study their impacts, and review possible defense methods.

4.1. Attack approaches

In a remote attack, the attackers send a flood of junk packets toward the service node over multiple hops (see Fig. 1). When a routing node receives the injected packets, it checks its routing table, finds the routing entry according to the destination addresses, and then forwards them. If the routing node traces back according to the source address, it may trace to the claimed source instead of the flooding source, or find that the claimed source is invalid. The reason why the attackers can still succeed in flooding without being detected is that discrepancies exist between routing and forwarding. For instance, even if secure routing protocols [21,24] are enforced in ad hoc networks, no further source verification is enforced in packet forwarding. Although the victim can identify the flooding sources with some intrusion detection systems, he may not be able to figure out where the packets come from.

4.2. Attack constraints

There are two types of constraints – self and cross congestion – often experienced by remote attacks.

4.2.1. Self congestion

Because a routing node shares the channel with other routing nodes in the same route, their transmissions interfere with each other. If an attacker injects packets very quickly, most packets will be buffered in upstream nodes and dropped later due to link failures. Our simulations show that attackers need to control the speed of packet generation to achieve the maximum throughput. The generation speed is measured by the *generation gauge*, which is the multiplication of the average period to generate one bit and the total channel bandwidth. In our simulations, the channel bandwidth is set to 1 Mbps. If a node generates attack load at 50 Kbps, i.e., it generates one bit every 2 μs on average, its generation gauge is 2. The quicker a node generates packets, the smaller the generation gauge.

Fig. 2 shows the relation between the achieved throughput of UDP traffic and the generation gauge in chain-like paths of different lengths. We depict the curves for 5-hop, 10-hop and 20-hop paths. In the figure, each curve has a peak. The slope at the right side of the peak illustrates a normal situation which has a slower packet generation, i.e., bigger generation gauge, which results in less throughput. The slope at the left side of the peak shows a special case which has faster packet generation and can reduce the throughput. Obviously, the maximum through-

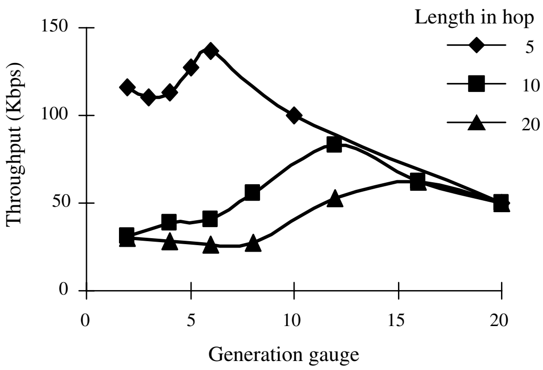


Fig. 2. UDP throughput in a chain-like path.

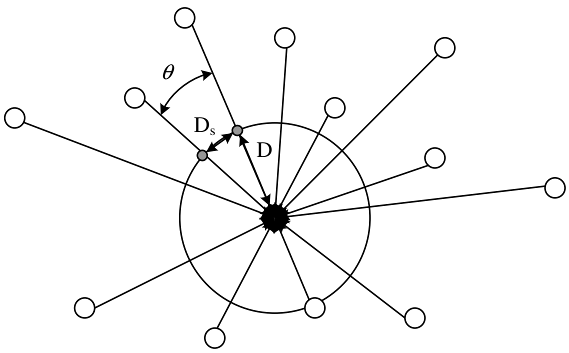


Fig. 3. Attack traffic collision.

put is achieved at the best generation gauge. Based on extensive simulations, we derive a heuristic rule as follows: For a single UDP path, the best generation gauge is:

- approximately 1.2 times of the hop number, if the length of the path is less than 12 hops; or
- around 15, if the length of the path is greater than 12 hops.

Due to self congestion, the longer a path is, the less maximum throughput the UDP traffic has. As illustrated in Fig. 2, if the path has 5 hops, the maximum throughput is around 145 Kbps. If the path has 10 hops, the maximum throughput is reduced to 80 Kbps. If the path has 20 hops, the maximum throughput is further reduced to 60 Kbps. Consequently, if one attacker is flooding a target from a very long distance, the traffic that can actually reach the target is less than 60 Kbps no matter how fast it generates packets.

4.2.2. Cross congestion

Cross congestion is another constraint, where different traffic flows interfere with each other. Consider Fig. 3 where all attackers send traffic toward the target in the center. Assume that all flooding sources are far away from each other, and able to find the best routes which directly point to the target. If the sensing distance is D_s and the average angle between every two closest routes is θ, at least one collision takes place at a location whose distance from the target satisfies $D \geqslant \frac{D_s}{2\sin\frac{\theta}{2}}$. In other words, at the distance D from the target, a maximum of $N_D = \frac{\pi}{\arcsin(D_s/2D)}$ flows can go through toward the target without collision.

In the target's sensing range, at most 6 flows do not interfere with each other. If the flooding nodes are 3 hops away from the target, each node can flood at 150–200 Kbps, and the total flooding traffic toward the service node can consume a channel capacity of 1 Mbps. If the flooding nodes are far away from the target, for example, more than 15 hops away, we need to consider the maximum throughput of a single UDP flow discussed in Section 4.2.1. Assume that the attackers are smart enough to select proper flooding topology so that the flooding flows do not interfere with each other before reaching the target. Sixteen flooding nodes may be needed, since each of them can only get 50–70 Kbps of flooding traffic to reach the target. In reality, however, because ad hoc routes are random, the attackers can hardly select such a topology to avoid cross congestion. We use the simulations to study the impact of the number of flooding nodes on the target.

4.3. Simulations

NS2 [25] was used to model the simulations, which was configured as follows:

Communication model. We use the default model in NS2, i.e., the two-ray ground reflection model in the physical layer, the IEEE 802.11 as the MAC and PHY protocols for communications, a sensing range of 550 m, a transmission range of 250 m, and the channel capacity as 1 Mbps. For communications over multiple hops, AODV is used as the routing protocol.

Network topology. We simulate the attacks in a 4200 m × 4200 m network. The network is divided into 441 grids, each of which is a 200 m × 200 m square area. Inside each grid, a node is randomly placed. Under these conditions, the network topology is randomly generated for each simulation. We do not consider the movement of nodes in these simulations, because the motion of nodes is much slower than the dynamics of the network under attack. In an ad hoc network, the flooding nodes may be randomly distributed in the network. This is typically the case when some normal nodes are compromised by the attackers for flooding. On the other hand, attackers can intentionally deploy some flooding nodes in a ring circling the service node. For comparison, the ring is centered at the service node and has a radius of 1300 m. The flooding nodes are selected from the nodes on or close (within 200 m) to the ring.

Traffic model. The node in the middle of the network is the service node, also referred to as the server in our discussion. In each simulation, we use CBR agents to generate normal and flooding traffic. In each simulation, we randomly select 10, 20, or 40 nodes as flooding nodes sending traffic toward the service node. The flooding traffic starts 5 s after the normal traffic, and continues for 30 s. The load of a flooding flow is 20 Kbps, 50 Kbps, 100 Kbps, or 200 Kbps. In each simulation, all flooding streams have the same attack load. In an ad hoc network, the communication between two nodes may still be congested by the flooding traffic toward the service node. Hence, we study two patterns of normal traffic. One is the traffic that goes between the service node and normal nodes. We randomly set the direction of the traffic to or from the service node. The other type of normal traffic is the traffic between two randomly selected nodes.

Default traffic setting. We compare the attack impacts under various traffic parameters and patterns. However, if it is not mentioned, the following default traffic setting is applied. The normal traffic is generated by 20 randomly selected normal nodes and the service node. Ten normal nodes communicate with the service node, and the other 10 randomly communicate with other nodes. Eighty percent of the normal traffic uses TCP connections, and the remaining 20% uses UDP packets. All normal traffic flows have a load of 20 Kbps. The flooding nodes are randomly put in the network. The flooding traffic uses UDP packets.

4.3.1. Experimental design

Five factors that may affect the attacks were considered in this study. We consider four attack loads (20, 50, 100, and 200 Kbps), three numbers of flooding nodes (10, 20, and 40), two positions of flooding nodes (random and ring), two loads of normal traffic (20 and 50 Kbps), and two patterns of normal traffic (service and random). Hence, an experimental design with 96 cells was used to represent the combinations of all the factors. For each cell, four independent simulations were conducted. In total, there were 384 data points for the experiment.

We use the throughput loss of the normal traffic to measure the attack impacts. The throughput loss is defined as the percentage of the bits in all dropped legitimate packets over the total bits in all legitimate packets during the attacks. The higher the throughput loss, the less the normal traffic can reach its destination and thus the more damage the attacks cause. Each point of the throughput loss in the comparison figures is the average of the four independent simulations. Note that the throughput loss is related to many factors in the application layer, such as extra delay of the service due to retransmission of the lost packets or disconnection from the service node due to the loss of service request packets.

4.3.2. Computational results

Table 1 presents the results of an analysis of variance (ANOVA) for attack impacts. In an ANOVA test, the factors have significant influence on the measurements when the *P*-value is small (e.g., less than 0.005). More explanations on *P*-value can be

Table 1
ANOVA analysis of remote attacks

Main effect	Mean square	DF	*F*-value	Significance
Load of flooding traffic (A)	0.00640	3	0.40	0.753
No. of flooding nodes (B)	0.08763	2	5.49	**0.005**
Position of flooding nodes (C)	0.00101	1	0.06	0.802
Load of normal traffic (D)	0.06379	1	4.00	0.048
Pattern of normal traffic (E)	0.23149	1	14.50	**0.000**
Two-way interaction				
A * B	0.01595	6	1.00	0.429
A * C	0.00802	3	0.50	0.681
A * D	0.03819	3	2.39	0.072
A * E	0.01996	3	1.25	0.295
B * C	0.01764	2	1.10	0.335
B * D	0.02733	2	1.71	0.185
B * E	0.18589	2	11.64	**0.000**
C * D	0.00034	1	0.02	0.884
C * E	0.00083	1	0.05	0.820
D * E	0.00812	1	0.46	0.497

[*] DF: degree of freedom; $\alpha = 0.05$.

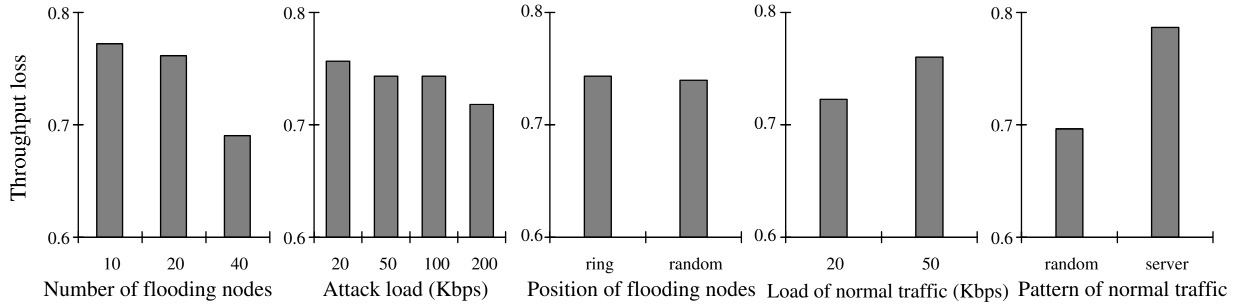


Fig. 4. Attack impacts of remote attacks under different factors.

found in [26]. Fig. 4 shows an overall evaluation of the main effects of these factors. The results indicate that, among these factors, the pattern of normal traffic is significant at $P < 0.001$ and the number of flooding nodes is significant at $P < 0.005$. Other factors show only slight influence.

The results indicate that if all normal nodes communicate with the service node, the damage from the flooding attack will be amplified. This shows that the normal traffic itself can cause packet loss in addition to the damage caused by the flooding traffic.

Also, we find that more flooding nodes leads to less throughput loss. For instance, the throughput loss drops from 77% for 10 flooding nodes to 69% for 40 flooding nodes. This indicates that cross congestion between flooding flows can significantly reduce the effective volume of flooding packets in the network. In this way, the remote attack is different from a traditional DDoS attack. As such, if the attacker uses 10 flooding nodes, he has a better chance of causing congestion in the network than if he uses 40 flooding nodes.

Although the results show that ring positioned flooding nodes may cause slightly more damage than randomly positioned flooding nodes, the impacts are not statistically significant. A higher load of normal traffic can cause higher throughput loss due to self congestion, but a higher load of flooding traffic slightly reduces the throughput loss. Consequently, in remote attacks, the most damage can be caused by a few flooding nodes with a low attack load.

Note that the difference in throughput loss under various factors is relatively small compared to the average throughput loss. In general, the high end of throughput loss is around 80%, while the low end of throughput loss is around 70%. Hence, in a remote attack, even if the attackers can control many flooding resources, the actual attack impact may not be greatly improved. In summary, in our simulations, 10 flooding nodes, each of them generating attack traffic at 20 Kbps, can cause the most damage on average.

4.3.3. Interactions among factors

We also evaluated the two-way interactions among the five factors. All the interactions, except the number of flooding nodes and the pattern of normal traffic, are insignificant.

Fig. 5 shows the throughput loss of the two patterns of normal traffic, different numbers of flooding

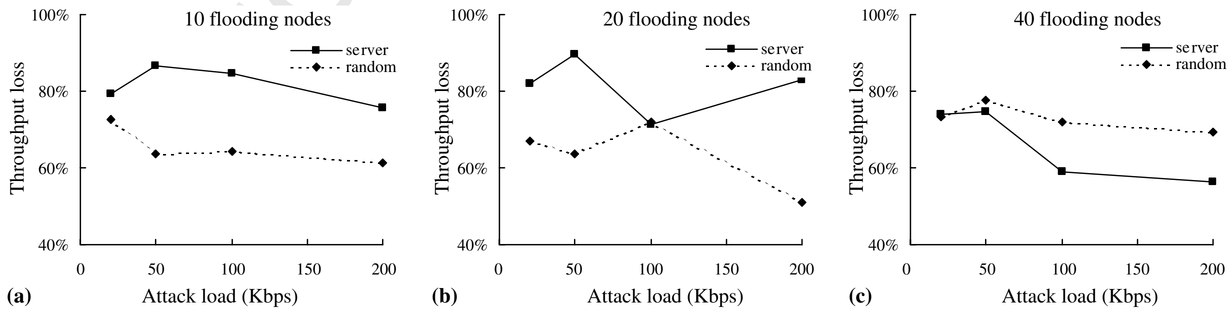


Fig. 5. Normal traffic patterns: with the service node or between random nodes. In each figure, the solid lines stand for the throughput loss of normal traffic that connects with the service nodes, and the dashed lines for the traffic between two randomly selected nodes.

nodes, and different attack loads. It is noted that when normal nodes communicate with the server, their traffic is more affected by the number of flooding nodes. When the number of flooding nodes is small as in Fig. 5(a), the normal traffic connecting with the service node can have more than 80% throughput loss. As the number of flooding nodes grows, the throughput loss drops to 70% or even less. In contrast, the throughput loss of random normal traffic keeps a similar dropping pattern from 70% to 60%, no matter how many flooding nodes are in the network. This comparison indicates that the flooding traffic mainly affects the service node when the number of the flooding nodes is small, because the flooding traffic concentrates in the vicinity of the service node, whereas in the other areas, the flooding traffic is not so intense. When the number of flooding nodes is large, the network is full of flooding traffic and thus any kind of normal traffic will be congested. In this situation, the throughput loss of both types of normal traffic in Fig. 5(c) is more similar than in others.

4.4. Defenses against remote attacks

Many defense approaches in the Internet have limitations when applied in an ad hoc network because they assume that: (a) attack hosts are end systems, (b) routers are trusted, and (c) victims are targets and vice versa. Unfortunately, all these assumptions are not necessarily true in ad hoc networks. Since attackers are inside an ad hoc network, they can send spoofed packets but claim the packets are forwarded. Routing nodes are not trustable either. Some routing nodes can be the attacker's colluders, and they can forward the flooding traffic. In the Internet, the network access can be controlled at the access point, such as by an ISP. However, in order to block a suspicious flooding source and its colluders in an ad hoc network, the routing nodes need to verify and filter the junk packets. In addition, an attack packet should be filtered as soon as possible once it is in the network, since it always has an impact on the area it goes through.

To prevent attackers from spoofing and flooding packets in an ad hoc network, hop-by-hop source authentication is needed so that every node participates in the protection of the network. Normal nodes can immediately detect and filter packets sent from malicious nodes. Yu et al. [27] proposed distributing a credential to the routing nodes with the routing packets when a route is set up. Then, only the nodes in the route can verify the digital signature in the packets and only the source and the destination nodes of the route can use this route. This approach ensures that no one else can spoof the source node inside or outside the route. However, a route in an ad hoc network may frequently change, which results in verification failures. Gu et al. [28] proposed another hop-by-hop source authentication approach to ensure that a packet can be verified when a route is changed. In this approach, the routing node at which a new route diverges from the old route takes the responsibility of authenticating the packets. The routing nodes in the new route can then verify the packets based on the new authentication information.

5. Local attacks

In this section, we analyze the characteristics of local attacks, study their impacts, and preview possible defense methods.

5.1. Attack approaches

In a local attack, the attackers send flooding traffic to their neighbor nodes to affect the traffic through the neighbor nodes (see Fig. 1). One advantage of local attacks is that the flooding nodes do not need to send the traffic over multiple hops. Thus, the flooding nodes do not rely on other routing nodes. Furthermore, the flooding nodes experience less self congestion, since the flooding traffic only goes through one hop. The flooding nodes also have less cross congestion, especially when two flooding nodes are far away from each other and cannot sense each other. The attack is effective only if the normal traffic goes through the flooding area. Greedy attackers may attack a lot of areas to make the maximum impact on the whole network instead of a single node.

One major problem of local attacks is that the flooding node needs to compete for the channel with normal nodes. The flooding node can congest others by composing large packets [29,30,17]. When a normal node is suppressed by a flooding node and unable to get sufficient bandwidth, it not only has to defer the transmission of its packets, but also has limited time to accept packets from other nodes. Other nodes may think the node is malfunctioning and the link to this node may be conceived as a failure. This will trigger other nodes to break routes going through this node or drop packets directed to this node. We will use simulations to study the complicated attack impacts.

5.2. Attack constraints

In a local attack, a flooding node only has a direct impact on the area in its vicinity. Hence, a local attack concerns how the flooding nodes may be deployed and how serious the attack is. For analysis purposes, we first observe the channel at a location x for a period of time T. During this period, it takes $t_{tr}(x)$ for transmission in the channel. Of $t_{tr}(x)$, $t_{norm}(x)$ is allocated for normal traffic. Then, define normal traffic density at location x, $D_{norm}(x) = \frac{\frac{t_{norm}(x)}{T}}{\int_S \frac{t_{tr}(x)}{T}dx}$, where S means the whole network.

The damage of a local attack can be measured as $M = 1 - \int_S D_{norm}(x)dx$. Because $t_{norm}(x) \leqslant t_{tr}(x)$, $\int_S D_{norm}(x)dx \leqslant 1$. If there is no attack, $t_{norm}(x) = t_{tr}(x)$ and thus $\int_S D_{norm}(x)dx = 1$ and $M = 0$, i.e., damage is zero. If normal transmission is totally disabled, $t_{norm}(x) = 0$ and $t_{tr}(x)$ is for the attack traffic only. In this case, $\int_S D_{norm}(x)dx = 0$ and $M = 1$, i.e., the network is 100% damaged.

It is very complicated to measure $t_{tr}(x)$ and $t_{norm}(x)$ in an attack, because (a) routes are highly dynamic under attack due to link failure, (b) the network traffic may be re-distributed due to route changes, and (c) the effect of the attack traffic on the normal traffic is determined by their interaction and thus is uncertain due to the first two reasons. However, it is possible to study some properties with simplified models. Assuming N compromised nodes can disable their vicinities 100% once they start an attack, then the damage (before the normal traffic is re-distributed) is:

$$M = 1 - \int_S D_{norm}(x)(1 - d(x))dx,$$

where $d(x)$ is a damage ratio, and $0 \leqslant d(x) \leqslant 1$. At location x, $d(x) = 1$ if x is inside the attack area of any attack host; otherwise, $d(x) = 0$, i.e., no damage to this location. If the flooding nodes are randomly distributed in the network, we can derive the average damage as $E(M) = 1 - \int_S D_{norm}(x)(1 - E(d(x)))dx$. When the normal traffic is uniformly distributed in an ad hoc network, i.e., $D_{norm}(x) = \frac{1}{S}$ and the attackers can congest area s, it is not difficult to prove that the damage is $M = \frac{s}{S}$, which indicates that the damage is proportional to the congested area in a network with uniformly distributed traffic. Hence, it conforms to our common sense that an attacker may want to deploy as many attack hosts as possible and assign each attack host to a non-overlapped area in a local attack.

5.3. Simulations

We use the same experiment as in Section 4.3, except all flooding nodes only send packets to one of its neighbors, to examine the characteristics of the local attacks. All flooding nodes are randomly selected from its neighbor nodes.

5.3.1. Computational results

Table 2 presents the results of an ANOVA for attack impacts. Fig. 6 shows an overall evaluation of the main effects. The results indicate that the pattern and load of normal traffic are significant at $P < 0.001$, and the position of flooding nodes is significant at $P < 0.05$. These three factors can have significant influence on the attack. The impacts of other factors are not statistically significant. Note that in both remote and local attacks, the impact from the pattern of normal traffic is significant. This indicates that an ad hoc network is vulnerable to all kinds of traffic. If the network is full of normal traffic, the result will be similar to a DDoS attack. From the viewpoint of the attackers, a good DDoS attack strategy is to make use of the normal traffic.

Table 2
ANOVA analysis of local attacks

Main effect	Mean square	DF	*F*-value	Significance
Load of flooding traffic (A)	0.02299	3	1.34	0.269
No. of flooding nodes (B)	0.03921	2	2.29	0.110
Position of flooding nodes (C)	0.11108	1	6.48	**0.013**
Load of normal traffic (D)	0.80994	1	47.27	**0.000**
Pattern of normal traffic (E)	1.67708	1	97.87	**0.000**
Two-way interaction				
A * B	0.01847	6	1.08	0.385
A * C	0.01741	3	1.02	0.392
A * D	0.02985	3	1.74	0.168
A * E	0.13395	3	7.82	**0.000**
B * C	0.00403	2	0.24	0.791
B * D	0.01508	2	0.88	0.420
B * E	0.11877	2	6.93	**0.002**
C * D	0.00641	1	0.37	0.543
C * E	0.11989	1	7.00	**0.010**
D * E	0.01576	1	0.92	0.341

* DF: degree of freedom; $\alpha = 0.05$.

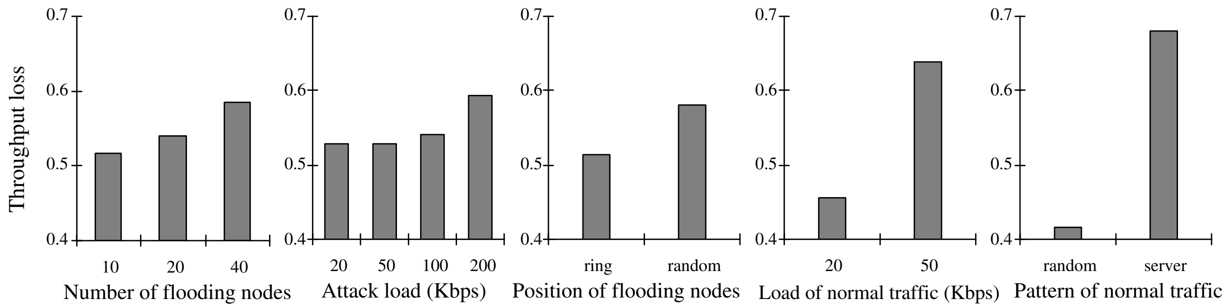


Fig. 6. Attack impacts in local attacks under different factors.

The attackers only need to deploy the flooding nodes in an area where normal traffic is not intense.

The load of normal traffic in a local attack is also a main factor. This indicates that the ability of a node to compete for the channel in a local attack is an important factor that determines what portion of the channel the node can obtain in a congestion situation. In a remote attack, the importance of this ability is reduced due to other problems in multi-hop transmission, such as exposed nodes and link failure [31].

A local attack differs from a remote attack in that the position of flooding nodes is one of the main factors. In a remote attack, since flooding traffic goes through multiple hops, the positions of the flooding nodes have less influence on where the traffic can go. In a local attack, one hop flooding traffic can only affect the nearby traffic. Hence, the attackers may want to deploy the flooding nodes uniformly in the network, if they can control the positions of the flooding nodes.

Although other factors show little influence on the attack, they exhibit some properties different from in remote attacks. First, in local attacks, the attack impacts are increased with an increased number of flooding nodes. Since the flooding traffic in the local attacks suffers less from self and cross congestions, more flooding nodes obviously can cause more damage to the network. Second, higher attack load in local attacks can cause more damage to the network. In a local attack, the most damage is caused when 40 flooding nodes are deployed in the network and each node floods at the highest rate. Finally, on average, the throughput loss in local attacks (0.55 ± 0.23) is less than that in remote attacks (0.74 ± 0.15). Note that when the network is crowded with flooding nodes, the gap in throughput losses can be reduced so that both types of attacks have similar impacts.

5.3.2. Interactions among factors

Since the attack impact in a local attack is mainly determined by how large an area is flooded by the attackers, the interactions among factors are also different from those in a remote attack. Our results indicate that the pattern of normal traffic has interaction with the load of flooding traffic, the number of flooding nodes, and the position of flooding nodes.

Fig. 7 shows that when normal nodes communicate with the service node, the flooding traffic has only a slight influence on the attack impacts. The average throughput loss of normal traffic is in a small range around 60% under different numbers of flooding nodes and different attack loads. Since in this sit-

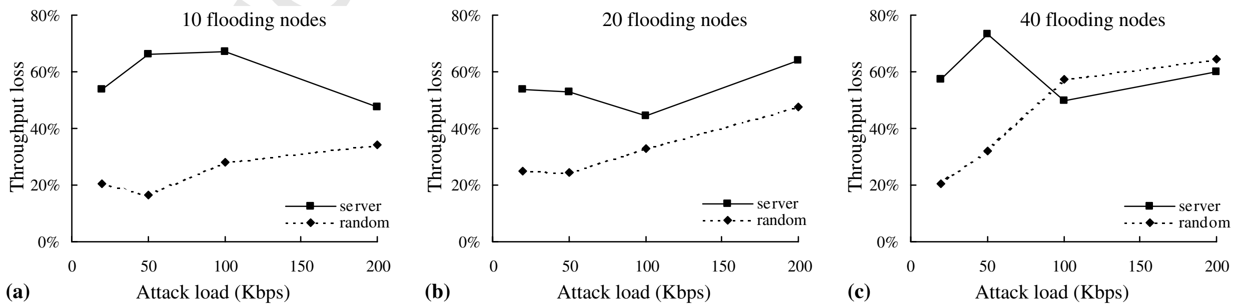


Fig. 7. Normal traffic patterns: with the service node or between two random nodes. In each figure, the solid lines stand for the throughput loss of the normal traffic that connects with the service nodes, and the dashed lines for the traffic between two randomly selected nodes.

uation, the normal traffic aggregates in the vicinity of the service node, the normal traffic flows suffer from cross congestion between themselves. The flooding nodes only cause additional damage to the normal traffic.

On the other hand, the random normal traffic has less cross congestion, and is thus more affected by the flooding traffic. Fig. 7(a) shows that the throughput loss of random normal traffic grows from 20% to 34% as the attack load increases. In Fig. 7(b) the throughput loss grows from 22% to 42% and in Fig. 7(c) the throughput loss grows from 20% to 61%. However, the throughput loss of random normal traffic is generally less than that of the normal traffic connecting with the service node. In the simulations, if the attack load is low, at 20 Kbps, the throughput loss of random normal traffic is only around 20%. The chance that the random normal traffic is affected by the flooding traffic is also influenced by the number of flooding nodes. The high end of the range of throughput loss of random normal traffic grows as the number of flooding nodes increases, especially when the attack load is high, at 200 Kbps. In Fig. 7(a), the high end of the range of throughput loss of random normal traffic is only 34% while in Fig. 7(c), the high end of the range reaches 61%.

5.4. Defense against local attacks

It is more difficult to prevent a malicious node from sending flooding packets through one hop, since no routing node is needed to forward junk packets in a local attack. If the number of flooding nodes is small, a routing node can redirect normal traffic to circle around the congested area. Wood et al. [32] proposed the JAM approach for letting nodes detect and avoid a jammed area. The idea can also be applied to protect normal traffic in a local DDoS attack. Normal nodes can first detect the congested area according to the frequency of link failure, the growing packet number in routing queues, etc. If a congested area is detected, normal nodes can forward packets to other nodes not in the congested area. However, the above approach is valid only if the majority of the network is not congested. When the number of flooding nodes is large, the whole network may be under attack. Then it is hard for a normal node to find another node not in a congested area.

Zhang et al. [33] proposed an intrusion detection architecture, in which all nodes monitor transmissions in their neighborhood and cooperate with their neighbor nodes to exchange intrusion detection information in order to detect the malicious node. Marti et al. [34] proposed using a watchdog to detect the attacking nodes. Basically, a normal node eavesdrops on its next hop to check whether its next hop forwards the packets that are received from the normal node. After detecting malicious nodes, the normal node uses a path rater to exclude the malicious node from its routes. In a clustered ad hoc network, a cluster head is elected for monitoring data traffic within the transmission range [35]. All of these intrusion detection approaches require nodes to monitor the transmissions in their neighboring areas. However, a malicious node may use a directional antenna for transmission in order to avoid monitoring. Also, a malicious node may ask other malicious nodes to circumvent its transmission area. Hence, monitoring nearby transmissions may not be practical in this kind of adversary environment. Furthermore, the detection relies on trusted neighboring nodes. They assume that a trusted node will honestly report misbehavior. However, a malicious node can ask another neighboring node to lie and deceive defenders.

6. Conclusion

DDoS attacks are already a serious threat to the Internet. In this paper, we show that DDoS attacks are also a serious threat to ad hoc networks and are more difficult to deal with in ad hoc networks. We studied the attack impacts of two types of DDoS attacks and compared important factors that influence the attacks. We find that a remote attack is a more effective and efficient method for DDoS attackers to damage the network. More flooding nodes and higher attack load cannot increase, but even reduce the attack impacts in a remote attack. On the other hand, local attacks need more resources than remote attacks. The damage in a local attack increases if more flooding nodes send traffic at a higher attack load in the network. We also find that the normal traffic has attack impacts on itself, and the DDoS attacks simply bring additional damage to the network.

Although many approaches to defend against DDoS attacks in the Internet have been developed, they cannot be directly applied to prevent DoS attacks in ad hoc networks. Several defense approaches against DoS attacks in ad hoc networks have also been proposed, but the dynamic behavior of congestion and the complication of DoS attacks in ad hoc networks deserve more investigation. This research explored the properties of area-congestion-based DDoS attacks, which lays the necessary foundation for developing more effective defense strategies against DDoS attacks in ad hoc networks.

Acknowledgement

This work was supported by NSF ANI-0335241, NSF CCR-0233324, and Department of Energy Early Career PI Award.

References

[1] P. Ferguson, D. Senie, Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing, RFC 2267 (1998).

[2] S. Savage, D. Wetherall, A. Karlin, T. Anderson, Practical network support for IP traceback, in: Proceedings of ACM SIGCOMM, 2000, pp. 295–306.

[3] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, S. Shenker, Controlling high bandwidth aggregates in the network, ACM SIGCOMM Computer Communications Review 32 (3) (2002) 62–73.

[4] J. Mirkovic, G. Prier, P. Reiher, Attacking DDoS at the source, in: Proceedings of IEEE ICNP, 2002, pp. 312–321.

[5] A. Yaar, A. Perrig, D. Song, Pi: a path identification mechanism to defend against DDoS attacks, in: Proceedings of IEEE Symposium on Security and Privacy, 2003, pp. 93–107.

[6] A. Yaar, A. Perrig, D. Song, SIFF: a stateless Internet flow filter to mitigate DDoS flooding attacks, in: IEEE Symposium on Security and Privacy, 2004, pp. 130–143.

[7] CERT advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks. Available from: <http://www.cert.org/advisories/CA-1996-21.html> (1996).

[8] CERT advisory CA-1998-01 smurf IP denial-of-service attacks. Available from: <http://www.cert.org/advisories/CA-1998-01.html> (1998).

[9] CERT advisory CA-1996-01 UDP port denial-of-service attack. Available from: <http://www.cert.org/advisories/CA-1996-01.html> (1996).

[10] T. Aura, P. Nikander, J. Leiwo, DoS-resistant authentication with client puzzles, in: Proceedings of Security Protocols Workshop 2000, Lecture Notes in Computer Science, Vol. 2133, Cambridge, UK, 2000, pp. 170–181.

[11] S.M. Bellovin, Security problems in the TCP/IP protocol suite, ACM SIGCOMM Computer Communication Review 19 (2) (1989) 32–48.

[12] J. Ioannidis, S.M. Bellovin, Implementing pushback: Router-based defense against DDoS attacks, in: Proceedings of NDSS (2002).

[13] J. Li, J. Mirkovic, M. Wang, P. Reiher, L. Zhang, SAVE: source address validity enforcement protocol, in: Proceedings of IEEE Infocom, vol. 3, 2002, pp. 1557–1566.

[14] J. Mirkovic, P. Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review 34 (2) (2004) 39–53.

[15] A. Perrig, J. Stankovic, D. Wagner, Security in wireless sensor networks, Communications of the ACM 47 (6) (2004) 53–57.

[16] J. Bellardo, S. Savage, 802.11 Denial-of-service attacks: real vulnerabilities and practical solutions, in: Proceedings of USENIX Security Symposium, Washington DC, 2003, pp. 15–28.

[17] Q. Gu, P. Liu, C.-H. Chu, Tactical bandwidth exhaustion in ad hoc networks, in: Proceedings of the 5th Annual IEEE Information Assurance Workshop, West Point, NY, 2004, pp. 257–264.

[18] C. Wullems, K. Tham, J. Smith, M. Looi, Technical summary of denial of service attack against IEEE 802.11 DSSS based wireless LANs, Tech. rep., Information Security Research Centre, Queensland University of Technology, Brisbane, Australia (2004).

[19] N. Borisov, I. Goldberg, D. Wagner, Intercepting mobile communications: the insecurity of 802.11, in: Proceedings of ACM MobiCom, 2001, pp. 180–189.

[20] I. Aad, J. Hubaux, E. Knightly, Denial of service resilience in ad hoc networks, in: Proceedings of ACM MobiCom, 2004.

[21] Y.-C. Hu, A. Perrig, D.B. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, in: Proceedings of ACM MobiCom, 2002, pp. 12–23.

[22] Y.-C. Hu, A. Perrig, D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in: Proceedings of ACM workshop on Wireless security, 2003, pp. 30–40.

[23] P. Ning, K. Sun, How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols, in: Proceedings of the 4th Annual IEEE Information Assurance Workshop, West Point, 2003, pp. 60–67.

[24] Y.-C. Hu, D. Johnson, A. Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, in: Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications, 2002, pp. 3–13.

[25] NS2, The network simulator. Available from: <http://www.isi.edu/nsnam/ns/> (2004).

[26] R.L. Ott, M.T. Longnecker, An introduction to statistical methods and data analysis, 5th ed., Duxbury Press, 2000.

[27] W. Yu, K.R. Liu, Defense against injecting traffic attacks in cooperative ad hoc networks, in: Proceedings of IEEE Globecom, 2005.

[28] Q. Gu, P. Liu, S. Zhu, C.-H. Chu, Defending against packet injection attacks in unreliable ad hoc networks, in: Proceedings of the IEEE Globecom, 2005.

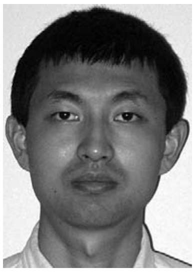
[29] H. Chhaya, S. Gupta, Throughput and fairness properties of asynchronous data transfer methods in the IEEE 802.11 MAC protocol, in: Proceedings of the 6th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, vol. 2, 1995, pp. 613–617.

[30] M. Heusse, F. Rousseau, G. Berger-Sabbatel, A. Duda, Performance anomaly of 802.11b, in: Proceedings of the IEEE Infocom, 2003, pp. 836–843.

[31] Z. Fu, P. Zerfos, K. Xu, H. Luo, S. Lu, L. Zhang, M. Gerla, The impact of multihop wireless channel on TCP throughput and loss, in: Proceedings of the IEEE Infocom, vol. 3, San Francisco, 2003, pp. 1744–1753.

[32] A. Wood, J. Stankovic, S. Son, JAM: a jammed-area mapping service for sensor networks, in: Proceedings of the 24th IEEE Real-Time Systems Symposium, 2003, pp. 286–297.

[33] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the ACM MobiCom, 2000, pp. 275–283.
[34] S. Marti, T.J. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the ACM MobiCom, ACM Press New York, NY, USA, Boston, Massachusetts, United States, 2000, pp. 255–265.
[35] Y.-A. Huang, W. Lee, A cooperative intrusion detection system for ad hoc networks, in: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003, pp. 135–147.



Qijun Gu is an assistant professor in Department of Computer Science, Texas State University, San Marcos. He received the PhD degree in Information Sciences and Technology from Pennsylvania State University in 2005. His research interests include wireless/mobile computing, denial of service, key management, ad hoc network, networking optimization, P2P sharing system.

Peng Liu is now an assistant professor of Information Sciences and Technology at Penn State University and the director of Cyber Security Lab. He received his BS and MS degree from the University of Science and Technology of China. He received his PhD degree from George Mason University in 1999. His research interests are in computer and network security. He has published a monograph and about 80 referred technical papers. He is the proceedings chair of the 2003 and 2004 ACM Conference on Computer and Communications Security. He is a program committee member of more than 35 conferences (e.g., WWW 2004, CCS 2006, INFOCOM 2007), and a referee for about 20 journals (e.g., ACM Transactions on Information and Systems Security). He is a recipient of the United States DOE Early CAREER Award.

Chao-Hsien Chu is an associate professor of Information Sciences and Technology and the executive director of the Center for Information Assurance at Pennsylvania State University. He received a PhD in Business Administration from Penn State. His current research interests are in communication networks design, information assurance and security (especially in wireless security, intrusion detection, and cyber forensics), and intelligent technologies (fuzzy logic, neural network, genetic algorithms, etc.) for data mining (e.g., bioinformatics, privacy preserving).